MICTSETA

118986 CYBERSECURITY ANALYST

EISA - 3

PRACTICAL - ASSESSMENT

New Assessment 3: Ransomware Incident Response

Scenario: Ransomware encrypts files on file server (192.168.20.10). Ransom note demands BTC; backups intact but untested. IT Manager activates IR plan amid business halt.

Task 1: Initial Detection & Isolation (20 Marks)

Aligns with ELO 1: Analyse, identify and solve security risks.

Question 1.1 (Practical Task):

Use Volatility on memory dump (ransomware.mem) to detect injected processes. Provide command. Identify ransomware indicators (e.g., Cobalt Strike beacon).

Rubric: Initial Detection & Isolation (20 Marks)

Criterion	Description	Marks
Command Accuracy	Exact Volatility command with profile/filter.	/5
Indicator Identification	Detects injected process/C2 IOCs.	/5
Risk Analysis	Rates "High" with persistence/lateral details.	/5
Alignment to ELO 1	Ties to isolation steps (e.g., net stop).	/5
Total: /20	Excellent (16-20): Full memory forensics.	Good (11-15): Basic process list.

Task 2: Log Analysis & Attribution (25 Marks)

Aligns with ELO 3: Execute ethical cybersecurity monitoring.

Question 2.1 (Practical Task):

Capture Sysmon logs; filter for encryption events. Use Wireshark on pcap for exfil. Extract TTPs.

Task 3: Containment & Eradication (30 Marks)

Identify: Ransomware encryption. Block: iptables -A INPUT -s 45.67.89.10 -j DROP. Rate-limit: Fail2ban jail on RDP. Policy: EDR deployment > blocks.

Task 4: Recovery & Lessons Learned (25 Marks)

Backup: rsync -a --delete /shares/ /mnt/backup/shares_$(date +%F). Incremental faster daily. Cloud: Rclone to Azure ensures Availability post-wipe.

Rubric: Log Analysis & Attribution (25 Marks)

Criterion	Description	Marks
Filter Commands	Accurate Sysmon/Wireshark filters.	/6
TTP Extraction	Identifies LOLBIN/exfil/C2.	/6
Attribution	Links to known group (e.g., TA505).	/6
Alignment to ELO 3	Recommends SIEM rules.	/7
Total: /25	Excellent (20-25): Chain-of-evidence.	Good (14-19): Partial logs.

New Assessment 4: Cloud Misconfiguration Audit

Scenario: AWS account (account ID: 123456789012) exposes S3 buckets publicly. IAM users have * policies. Compliance audit flags POPIA violations.

Task 1: Configuration Scan & Risk ID (20 Marks)

Aligns with ELO 1: Analyse, identify and solve security risks.

Question 1.1 (Practical Task):

Use Pacu on AWS creds to scan for misconfigs. Command? Identify high-risk issues (e.g., public bucket).

Rubric: Configuration Scan & Risk ID (20 Marks)

Criterion	Description	Marks
Command Accuracy	Pacu session/enumerate commands.	/5
Misconfig ID	Lists public S3/IAM issues.	/5

Criterion	Description	Marks
Risk Analysis	Quantifies "High" (e.g., R10M fine).	/5
Alignment to ELO 1	Remediation path outlined.	/5
Total: /20	Excellent (16-20): Full enum.	Good (11-15): Basic scan.

Task 2: Access Logging & Monitoring (25 Marks)

Aligns with ELO 3: Execute ethical cybersecurity monitoring.

Question 2.1 (Practical Task):

Enable CloudTrail; query Athena for suspicious API calls. Filter/extract.

Task 3: Hardening & Least Privilege (30 Marks)

Attack: IAM over-priv. Block: aws iam delete-policy-version --policy-arn arn:aws:iam::123456789012:policy/OverPerm. SCP rate-limit. Policy: Just-In-Time access > static roles.

Task 4: Backup & DR (25 Marks)

Backup: aws s3 sync s3://company-data /mnt/backup --storage-class DEEP_ARCHIVE. Incremental via versioning. Cloud-native: Cross-region replication upholds CIA Availability.

Rubric: Access Logging & Monitoring (25 Marks)

Criterion	Description	Marks
Query/Filter	Athena/CloudTrail accurate filters.	/6
Event Extraction	Suspicious API/user details.	/6
Monitoring Setup	Enables GuardDuty/Alarms.	/6
Alignment to ELO 3	POPIA audit trails.	/7
Total: /25	Excellent (20-25): Proactive alerts.	Good (14-19): Basic query.

MICTSETA | Media, Information And Communication Technologies Sector Education And Training Authority

SHAPING SKILLS, PIONEERING INDUSTRIES, EMPOWERING FUTURES